CLAIMS

We claim:

1. A method for providing access services, comprising the steps of:

receiving user session state information for a first user;

receiving resource request information for a first resource;

receiving a request to authorize said first user to access said first resource, said request to authorize is from an application without a web agent front end; and

attempting to authorize said first user to access said first resource without requiring said first user to re-submit authentication credentials.

2. A method according to claim 1, wherein:

said user session state information is a session token from a cookie stored on a client for said first user.

3. A method according to claim 1, wherein:

said user session state information is from a cookie stored on a client for said first user;

said user session state information is encrypted; and

said step of receiving user session state information includes decrypting said user session state information.

4. A method according to claim 3, further including the steps of:

receiving a request from said application for unencrypted data from said user session state information; and

providing said unencrypted data from said user session state information to said application, said application does not have access to a key to decrypt said user

session state information.

5. A method according to claim 4, wherein:

said unencrypted data includes an identity for said first user.

6. A method according to claim 1, wherein:

said user session state information is a session token from a cookie stored on a client for said first user, said session state information was created by an access system; and

said access system performs said step of attempting to authorize.

7. A method according to claim 1, wherein:

said user session state information is a session token from a cookie stored on a client for said first user, said user session state information was created by an access system and provided to said application by said access system;

said application caused said session token to be stored in said cookie; and

said access system performs said step of attempting to authorize.

8. A method according to claim 1, wherein said user session state information includes:

an identity for said first user;

an authentication level for said first user; and

a session start time for said first user.

9. A method according to claim 1, wherein said resource request information includes:

an identification of a resource type;

an identification of a resource; and

an identification of an operation.

10. A method according to claim 1, wherein said resource request information includes:

an identification of a resource type;

an identification of a resource;

an identification of an operation; and

query string information.

11. A method according to claim 1, wherein said resource request information includes:

an identification of a resource type;

an identification of a resource;

an identification of an operation; and

post data information.

12. A method according to claim 1, wherein:

said web agent front end is a Web Gate.

13. A method according to claim 1, wherein:

said step of attempting to authorize is based on said user session state information and said resource request information.

14. A method according to claim 1, further comprising the steps of:

creating a resource request object, said resource request object represents a request to access said first resource; and

creating a user session object, said user session object represents said first user after said first user has been authenticated.

15. A method according to claim 1, further comprising the steps of:

determining whether said first resource is protected;

determining an authentication scheme for said first resource; and

determining whether said authentication scheme is satisfied based on said user session state information.

16. A method according to claim 15, further comprising the steps of:

making available to said application an indication of whether said first resource is protected; and

making available to said application an indication of said authentication scheme.

17. A method according to claim 1, further comprising the step of:

determining one or more authentication actions for said first resource.

18. A method according to claim 17, further comprising the step of:

making available to said application an indication of said one or more authentication actions for said first resource.

19. A method according to claim 17, further comprising the step of:

performing at least one of said authentication actions for said first resource.

20. A method according to claim 1, further comprising the step of:

determining one or more authorization actions for said first resource.

21. A method according to claim 20, further comprising the step of:

making available to said application an indication of said one or more authorization actions for said first resource.

22. A method according to claim 20, further comprising the step of:

performing at least one of said authorization actions for said first resource.

23. A method according to claim 1, further comprising the step of:

determining one or more audit rules for said first resource.

24. A method according to claim 23, further comprising the step of:

making available to said application an indication of said one or more audit rules for said first resource.

25. A method according to claim 23, further comprising the step of:

performing at least one of said audit rules for said first resource.

26. A method according to claim 1, further comprising the step of:

allowing said first user to access said first resource if said first user is authorized to access said first resource.

27. A method for providing access services by an application without a web agent front end, comprising the steps of:

receiving an electronic request from a first user to access a first resource, said step of receiving includes receiving information from a cookie;

providing said information from said cookie to an access system interface;

and

requesting said access system interface to authorize said first user to access said first resource based on information from said electronic request from said first user and based on said information from said cookie.

28. A method according to claim 27, wherein:

said information from said cookie is encrypted.

29. A method according to claim 28, further comprising the steps of:

requesting unencrypted data from said information from said cookie, said request being made to said access system interface; and

receiving said unencrypted data from said access system interface.

30. A method according to claim 29, wherein:

said application does not have access to a key for decrypting said information from said cookie.

31. A method according to claim 27, further comprising the steps of:

requesting data from said information from said cookie, said request being made to said access system interface;

receiving said data from said access system interface; and

using said data for an access system service.

32. A method according to claim 27, wherein:

said information from said cookie was originally provided by a first web agent..

33. A method according to claim 27, wherein:

said information from said cookie was originally provided by said access system interface.

34. A method according to claim 27, further comprising the steps of:

determining whether said first resource is protected;

determining an authentication scheme for said first resource;

determining whether said authentication scheme is satisfied based on said information from said cookie; and

determining whether said first user is authorized to access said first resource.

35. A method according to claim 34, further comprising the step of:

allowing said first user to access said first resource if said first user is authorized to access said first resource.

36. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving user session state information for a first user;

receiving resource request information for a first resource;

receiving a request to authorize said first user to access said first resource, said request to authorize is from an application without a web agent front end; and

attempting to authorize said first user to access said first resource without requiring said first user to re-submit authentication credentials.

37. One or more processor readable storage devices according to claim 36, wherein:

said user session state information is from a cookie stored on a client for said first user;

said user session state information is encrypted; and

said step of receiving user session state information includes decrypting said user session state information.

38. One or more processor readable storage devices according to claim 37, wherein said method further comprises the steps of:

receiving a request from said application for unencrypted data from said user session state information; and

providing said unencrypted data from said user session state information to said application, said application does not have access to a key to decrypt said user session state information.

39. One or more processor readable storage devices according to claim 36, wherein:

said user session state information is a session token from a cookie stored on a client for said first user, said session state information was created by an access system; and

said access system performs said step of attempting to authorize.

40. One or more processor readable storage devices according to claim 36, wherein said method further comprises the steps of:

determining whether said first resource is protected;

determining an authentication scheme for said first resource;

determining whether said authentication scheme is satisfied based on said user session state information;

making available to said application an indication of whether said first resource is protected; and

making available to said application an indication of said authentication scheme.

41. One or more processor readable storage devices according to claim 36, wherein said method further comprises the steps of:

determining one or more authorization actions for said first resource; and

making available to said application an indication of said one or more authorization actions for said first resource.

42. One or more processor readable storage devices according to claim 36, further comprising the step of:

allowing said first user to access said first resource if said first user is authorized to access said first resource.

43. An apparatus, comprising:

a communication interface;

one or more storage devices; and

one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method comprising the steps of:

receiving user session state information for a first user,

receiving resource request information for a first resource,

receiving a request to authorize said first user to access said first

resource, said request to authorize is from an application without a web agent front end, and

attempting to authorize said first user to access said first resource without requiring said first user to re-submit authentication credentials.

44. An apparatus according to claim 43, wherein:

said user session state information is from a cookie stored on a client for said first user;

said user session state information is encrypted; and

said step of receiving user session state information includes decrypting said user session state information.

45. An apparatus according to claim 44, wherein said method further comprises the steps of:

receiving a request from said application for unencrypted data from said user session state information; and

providing said unencrypted data from said user session state information to said application, said application does not have access to a key to decrypt said user session state information.

46. An apparatus according to claim 43, wherein:

said user session state information is a session token from a cookie stored on a client for said first user, said session state information was created by an access system; and

said access system performs said step of attempting to authorize.

47. An apparatus according to claim 43, wherein said method further

comprises the steps of:

determining whether said first resource is protected;

determining an authentication scheme for said first resource;

determining whether said authentication scheme is satisfied based on said user session state information;

making available to said application an indication of whether said first resource is protected; and

making available to said application an indication of said authentication scheme.

48. An apparatus according to claim 43, wherein said method further comprises the steps of:

determining one or more authorization actions for said first resource; and

making available to said application an indication of said one or more authorization actions for said first resource.

49. An apparatus according to claim 43, further comprising the step of:

allowing said first user to access said first resource if said first user is authorized to access said first resource.

50. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method for providing access services by an application without a web agent front end, the method comprising the steps of:

receiving an electronic request from a first user to access a first resource, said step of receiving includes receiving information from a cookie;

providing said information from said cookie to an access system interface; and

requesting said access system interface to authorize said first user to access said first resource based on information from said request from said first user and based on said information from said cookie.

51. One or more processor readable storage devices according to claim 50, wherein:

said information from said cookie is encrypted; and

said method further comprises the steps of:

requesting unencrypted data from said information from said cookie, said request being made to said access system interface,

receiving said unencrypted data from said access system interface, and

using said unencrypted data for an access system service.

52. One or more processor readable storage devices according to claim 51, wherein:

said application does not have access to a key for decrypting said information from said cookie.

53. An apparatus, comprising:

a communication interface;

one or more storage devices; and

one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method for providing access services by an application

without a web agent front end, the method comprising the steps of:

receiving an electronic request from a first user to access a first resource, said step of receiving includes receiving information from a cookie,

providing said information from said cookie to an access system interface, and

requesting said access system interface to authorize said first user to access said first resource based on information from said request from said first user and based on said information from said cookie.

54. An apparatus according to claim 53, wherein:

said information from said cookie is encrypted; and

said method further comprises the steps of:

requesting unencrypted data from said information from said cookie, said request being made to said access system interface,

receiving said unencrypted data from said access system interface, and

using said unencrypted data for an access system service.

55. An apparatus according to claim 54, wherein:

said application does not have access to a key for decrypting said information from said cookie.

56. A method for providing access services, comprising the steps of:

authenticating a first user;

causing user session state information to be stored at a client for said first user;

authorizing said first user to access a first protected resource;

receiving a request from an application without a web agent front end to allow said first user to access a second protected resource, said step of receiving a request includes receiving said user session state information from said application;

allowing said first user to access said second protected resource without requiring said first user to re-submit authentication credentials, if said first user is authorized to access said second protected resource.

57. A method according to claim 56, wherein:

said user session state information is from a cookie stored on a client for said first user;

said user session state information is encrypted; and

said step of receiving includes decrypting said user session state information.

58. A method according to claim 57, further including the steps of:

receiving a request from said application for unencrypted data from said user session state information; and

providing said unencrypted data from said user session state information to said application, said application does not have access to a key to decrypt said unencrypted data from said user session state information.

59. A method according to claim 56, wherein:

said user session state information is a session token from a cookie stored on a client for said first user, said session state information was created by an access system; and

said access system performs said step of allowing.

60. A method according to claim 56, further comprising the steps of:

determining whether said second resource is protected;

determining an authentication scheme for said second resource;

determining whether said authentication scheme is satisfied based on said user session state information;

making available to said application an indication of whether said first resource is protected; and

making available to said application an indication of said authentication scheme.